www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 9 September 2013 Page No. 2750-2755

Risk aware and ALERT protocol for mitigating routing attacks in Mobile Ad hoc Networks

D. Francis Xavier Christopher[1], R.Nithya[2]

[1] Director, School of Computer Studies, RVS College of Arts and Science
Coimbatore, Tamil Nadu, India
christopher@rvsgroup.com

[2] Research Scholar, Department of Computer Science, RVS College of Arts and Science
Coimbatore, Tamil Nadu, India
nithyasiva28@gmail.com

Abstract: ***Mobile Ad Hoc Networks (MANET) has been highly vulnerable to attacks due to the dynamic nature of its network infrastructure. Among these attacks, the routing attacks getting more attention because it's changing the whole topology itself and it causes more damages to MANET. The existing algorithm not provides the anonymity protection and finding the malicious node with degree of evidence from the expert knowledge and detects the important factors for each node. In proposed method the ALERT protocol is developed for overcome the existing problem. ALERT protocol is mainly providing a high anonymity protection with low cost. Using proposed protocol the network fields are dynamically partitions into zones and zones are randomly chosen from the nodes as intermediate relay nodes, which form a non-traceable by anonymous route. Particularly in every routing step, a data sender or forwarder division the network field in order to disconnected itself and the destination into two zones. In the last step, the data are broadcast to k nodes in the destination zone providing k-anonymity to the destination. ALERT is also flexible to timing attacks and intersection attacks. In addition, the experiments demonstrate the effectiveness of proposed approach with the consideration of several performance metrics.***

Keywords: MANET, risk aware, dempster-shafer theory, anonymity, ALERT.

1. Introduction

Mobile Ad hoc Networks (MANET) area unit utilized to line up wireless communication in unprepared environments while not a predefined infrastructure or centralized administration. Therefore, MANET has been unremarkably deployed in adverse and hostile environments wherever central authority purpose isn't necessary. The vital characteristic of MANET is that the dynamic nature of its constellation which might be often modified attributable to the unpredictable quality of nodes. Furthermore, every mobile node in MANET plays a router role whereas transmission knowledge over the network. Hence, any compromised nodes beneath an adversary's management might cause vital injury to the practicality and security of its network since the impact would propagate in acting routing tasks. There is a unit another challenges and complexities:

(i) The scalability is needed in MANET because it is employed in military communications, as a result of the network grows consistent with the necessity, therefore every mobile device should be capable to handle the intensification of network and to accomplish the task.

(ii) MANET is infrastructure less network with no central administration. Every device will communicate with each alternative device. Therefore it becomes tough to notice and manage the faults. In MANET the mobile devices will move at random. The employment of this dynamic topology ends up in route changes, frequent network partitions and probably packet losses.

(iii) Every node within the network is autonomous. Therefore have the instrumentality for radio interface with completely different transmission or receiving capabilities in uneven links.

2. Routing attack

Attacks in MANETs can be classified into passive or active attacks [1]. In passive attacks the aggressor doesn't send any message, however simply listens to the channel. Passive attack area unit non unquiet however area unit data seeking, which can be important within the operation of a protocol. Active attacks could either be directed to disrupt the conventional operation of a particular node or target the operation of the full network. Attacks are often additional categorized as either outsider or insider attacks. With relevance the target, attacks may be additionally divided into information packet or routing packet attacks. In routing packet attacks, attackers couldn't only prevent existing ways from getting used, however additionally spoof nonexistent ways to lure information packets to them. Many studies are distributed on modeling MANET routing attacks. Routing attacks include black hole, fabrication, and modification of varied fields in routing packets (request message, reply message, and error message, etc.). Of these attacks could lead to serious network dysfunctions. A malicious node will disrupt the routing mechanism within the following easy ways: i) It changes the contents of a discovered route, ii)Modifies a route reply message, iii) Causes the packet to be born as an invalid packet; iv)It validates the route cache in additional nodes by advertising incorrect paths v) Refuses to participate with in the route discovery procedure; vi) It modifies the contents of a message packet or the route via that the information packet is mean to travel or behave ordinarily throughout the route discovery process however is born.

3. Proposed methodology

3.1 Routing protocol OLSR

The major task of the routing protocol is to construct routes to its destinations. Proactive routing protocols OLSR within which nodes get routes by periodic exchange of topology information with other nodes and maintain route information all the time. OLSR protocol achieves optimization through the use of multipoint relay (MPR) to provide an efficient flooding mechanism by reducing the number of transmissions required [2]. Each node declares its links and forward messages for their neighbors, only nodes selected as MPR nodes are dependable for advertising as well as forwarding an MPR selector list advertised by alternative MPRs.

Random packets were generated and transmitted among nodes without activating any of them as attackers. This replication can present the traffic patterns below the traditional circumstance. In OLSR any node can either modify the protocol messages before forwarding them or generate false messages or spoof an identity. Therefore the aggressor will abuse the properties of the choice algorithm to be selected as MPR. The most terrible case is the possible selection of the aggressor as the only MPR of a node that offer wrong information about the topology of a network (TC message) in order to disturb the routing operation.

Specific nodes were set as attackers which conducted malicious activities for their own profits. This simulation process can present the traffic patterns under the circumstance with malicious activities.

3.2. Dempster's Rule of Combination with Importance Factors (DRCIF)

Dempster-Shafer mathematical theories of proof are that the procedure to combination and summarize a corpus of evidences. Theorem1. Dempster's Rule of Combination with Importance Factors: Suppose Bel1 and Bel2 square measure belief functions over an equivalent frame with basic likelihood assignments money supply and money supply [3][4]. The IF of those evidences is IF1 and IF2. Then, perform outlined by

$$m'(\phi) = 0 \qquad (1)$$

and

$$m'(C, IF_1, IF_2) = \frac{\sum_{A_i \cap B_j = C} \left[m_1(A_i)^{\frac{IF_1}{IF_2}} \cdot m_2(B_j)^{\frac{IF_2}{IF_1}} \right]}{\sum_{C \subseteq \Theta, C \neq \phi} \sum_{A_i \cap B_j = C} \left[m_1(A_i)^{\frac{IF_1}{IF_2}} \cdot m_2(B_j)^{\frac{IF_2}{IF_1}} \right]}, \qquad (2)$$

for all nonempty could be a likelihood assignment for the combined proof.

DRCIF is non associative (trust all evidences equally) for multiple evidences. Therefore, for the case during which ordered data isn't accessible for a few instances, it's necessary to form the results of combination according to multiple evidences. It indicates that our extended Dempster-Shafer theory demands no further process value compared to a naive fuzzy-based technique. The algorithmic rule for combination of multiple evidences is built as follows:

Algorithm 1: MUL-EDS-CMB

```
INPUT: Evidence pool Ep
OUTPUT: One evidence
|Ep| = size of (Ep);
While |Ep| > 1 do
    Pick two evidences with the least IF in Evidence pool, named $E_1$ and $E_2$;
    Combine these two evidences,
        $\langle m_1 \oplus m_2, (IF_1 + IF_2)/2 \rangle$;
    Remove $E_1$ and E2 from Ep;
    Add E to Ep;
end
return the evidence in Ep.
```

3.3 Risk-aware response mechanism

Risk-aware response mechanism supported quantitative risk estimation and risk tolerance [5]. Rather than applying simple binary isolation of malicious nodes, this approach adopts an isolation mechanism during a temporal manner based on the risk value.

Each node in this system makes its own response decisions based on the evidences and its own individual benefits. Therefore, some nodes in MANET might isolate the malicious node; however others should confine cooperation with a result of high dependency relationships.

Collection of evidence: Intrusion Detection System (IDS) gives an attack alert with a confidence value and then Routing Table Change Detector (RTCD) runs to work out how many changes on routing table are caused by the attack.

Risk assessment: Alert confidence from IDS and routing table fixing data would be extra thought-about as freelance evidences for risk calculation and combined with the extended D-S theory. Risk of countermeasures is calculated additionally throughout a risk assessment part. Supported the danger of attacks and therefore the risk of countermeasures, the total risk of associate attack can be calculate.

Decision making: The adaptation call module provides a versatile response decision-making mechanism, that takes risk estimation and risk tolerance under consideration. To manage temporary isolation level, a user can set utterly totally different thresholds.

Intrusion response: Intrusion response offer the output from risk assessment and decision-making module, the corresponding response actions, together with routing table recovery and node isolation, area unit administered to mitigate attack damages throughout a distributed manner.

3.3.1 Response to Routing Attacks

Routing table recovery is an indispensable response and can perform the first response technique once lucky detection of attacks. Native routing recovery is performed by victim nodes that realize the attack and automatically recover its own routing table. World routing recovery involves with causing recovered routing messages by victim nodes and alter their routing table supported corrected routing information in real time by completely different nodes in MANET. Node isolation may even be the foremost intuitive due to stop any attacks from being launched by malicious nodes in MANET.

3.3.2 Risk Assessment

Since the attack response actions could cause a lot of damages than attacks, the risks of each attack and response ought to be calculable. We tend to classify the safety states of MANET into 2 categories: {Secure, Insecure}. In alternative words, the frame of discernment would be { ϕ, {Secure}, {Insecure}, {Secure, Insecure}}. Note that {Secure, Insecure} suggests that the safety state of MANET might be either secure or insecure, that describes the uncertainty of the safety state. Bel {Insecure} is employed to represent the risk of MANET.

a) Evidence collection

Evidence 1: the boldness of attack detection by the IDS is provided to handle the chance of the attack prevalence.

Evidence 2: This proof indicates the proportion of missing entries in routing table. Node isolation measure will cause potential deletion of entries from routing table of the node.

Evidence 3: This proof represents the proportion of fixing entries within the case of next hop being the malicious node.

Evidence 4: This proof shows the proportion of modified entries within the case of various next hop (not the malicious node) and also the same distance.

Evidence 5: This proof points out the proportion of fixing entries within the case totally different next hop (not the malicious node) and also the different distance. Just like proof four, each attacks and countermeasures may end in this proof. . The trail modification may additionally have an effect on routing value and transmission delay of the network.

b) Combination of Evidences

The combined proof for associate attack Semitic deity and also the combined proof for a measure global organization. Thus, BelA(Insecure) and BelC(Insecure) represent risks of attack (RiskA) and measure (RiskC), severally [6]. The combined evidences, Semitic deity and global organization are outlined in equivalent.

$$E_A = E_1 \oplus E_2 \oplus E_3 \oplus E_4 \oplus E_5 \tag{3}$$

$$E_C = E_2 \oplus E_4 \oplus E_5 \tag{4}$$

Where is Dempster's rule of combination with vital factors outlined in Theorem one

$$Risk = Risk_A - Risk_C = Bel_A(Insecure) - Bel_C(Insecure) \tag{5}$$

3.3.3 Adaptive Decision Making

It is supported quantitative risk estimation and risk tolerance. The response level is moreover separated into multiple bands. Every band is connected with associate degree isolation degree that presents a particular amount of the isolation action. The response level and band limits unit all determined in accordance with risk tolerance and can be modified once risk tolerance threshold changes.

The higher risk tolerance threshold (UT) would be related to permanent isolation response. The lower risk tolerance threshold (LT) would keep every node intact. The band between the UT and LT is claimed to the provisionary isolation response within that the isolation time (T) changes dynamically supported the numerous reply levels [7].

The value of lower risk tolerance threshold is zero initially if no additional information is on the market. It implies once the chance of attack is larger than the chance of isolation response, the isolation is required. If completely different information is on the market, it might be wont to regulate thresholds.

If the compromised node incorporates a high or low name level, the response module will intuitively regulate the chance tolerance thresholds consequently. If LT may well be a smaller amount than zero and risk of attack is larger than the chance of isolation, the response might in addition perform Associate in nursing isolation task to the malicious nodes.

The risk tolerance thresholds might even be dynamically adjusted by another issue like attack frequency. If the attack frequency is high, additional severe response action got to be taken to counter this attack by reducing the values of risk tolerance threshold and narrowing the vary between 2 risk tolerance thresholds.

3.4. ALERT routing mechanism

ALERT options a dynamic and unpredictable routing path that consists of variety of dynamically determined intermediate relay nodes. As shown within the higher a part of Figure 1, horizontally partition it into 2 zones A1 and A2 and vertically partition zone A1 to B1 and B2. After that, horizontally partition zone B2 into 2 zones. Such zone partitioning consecutively splits the tiniest zone in AN alternating horizontal and vertical manner. This partition method is called the hierarchical zone partition. ALERT uses the hierarchical zone partition and arbitrarily chooses a node within the partitioned off zone in every step as an intermediate relay node (i.e., knowledge forwarder), so dynamically generating hit and miss routing path for a message.

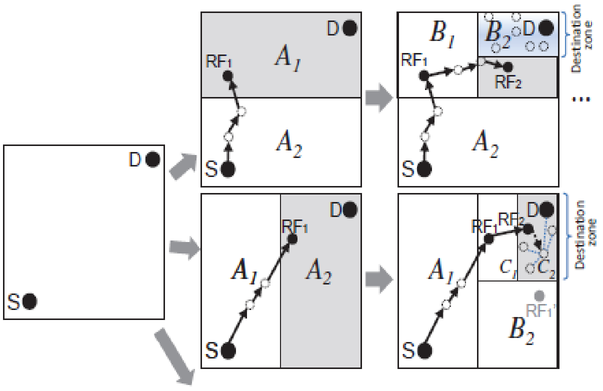

Figure 1: Samples of completely different zone partitions

Figure 2 shows AN example of routing in ALERT. The zone having k nodes wherever D resides the destination zone, denoted as ZD. k is employed to regulate the degree of obscurity protection for the destination. The shaded zone in Figure 2 is that the destination zone. Specifically, within the ALERT routing, every knowledge supply or forwarder executes the hierarchic zone partition. It 1st checks whether or not itself and destination square measure within the same zone. If so, it divides the zone as an alternative within the horizontal and vertical directions. The node repeats this method till it and ZD aren't within the same zone. It then arbitrarily chooses a foothold within the alternative zone referred to as temporary destination (TD), and uses the GPSR routing rules to send the info to the node closest to TD. This node is outlined as a random forwarder (RF).

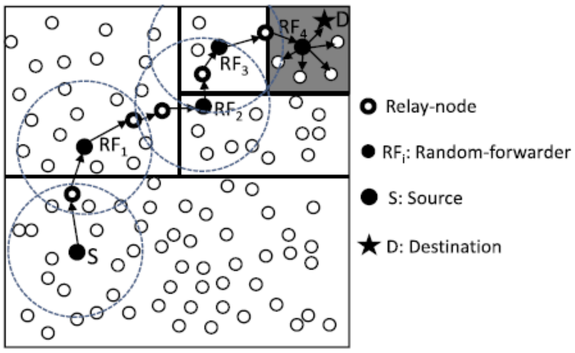

Figure 2: Routing among zones in ALERT

Given an S-D combine, the partition pattern in ALERT varies looking on the arbitrarily elect TDs and therefore the order of horizontal and vertical division that provides a much better obscurity protection. Figure 1 shows 2 doable routing methods for a packet pkt issued by sender S targeting destination D in ALERT. There are several alternative doable methods. Within the higher routing flow, knowledge supply S 1st horizontally divides the realm into 2 equal-size zones, A1 and A2, so as to separate S and ZD. S then arbitrarily selects the primary temporary destination TD1 in zone A1 wherever ZD resides. Then, S depends on GPSR (Greedy Perimeter unsettled Routing) to send pkt to TD1. GPSR makes greedy forwarding choices exploitation solely info a few router's immediate neighbors within the topology. The pkt is forwarded by many relays till reaching a node that can't realize a neighbor nearer to TD1. This node is taken into account to be the primary random-forwarder RF1. Once RF1 receives pkt, it vertically divides the region A1 into regions B1 and B2 so ZD and it square measure separated in 2 completely different zones. Then, RF1 arbitrarily selects successive temporary destination TD2 and uses GPSR to send pkt to TD2. This method is perennial till a packet receiver finds itself residing in ZD, i.e., a partitioned off zone is ZD having k nodes. Then, the node broadcasts the pkt to the k nodes. The lower a part of Figure 1 shows another routing path supported a unique partition pattern. Once S vertically partitions the complete space to separate itself from ZD, it arbitrarily chooses TD1 and sends pkt to RF1. RF1 partitions zone A2 into B1 and B2 horizontally so partitions B1 into C1 and C2 vertically, so it and ZD square measure separated. Note that RF1 might vertically partition A2 to separate itself from ZD in 2 zones however could opt for a TD any removed from the destination than the TD that resulted from the horizontal partition. Therefore, ALERT sets the partition within the various horizontal and vertical manners so as to confirm that a pkt approaches D in every step.

The destination node won't move secluded from its position throughout the info transmission, thus it will with success receive the info. During this style, the trade-off is that the obscurity protection degree and transmission delay. a bigger variety of hierarchies generate additional routing hops, that will increase obscurity degree however conjointly will increase the delay. to confirm the delivery of packets, the destination sends a confirmation to the supply upon receiving the packets. If the supply has not received the confirmation throughout a predefined fundamental measure, it'll resend the packets.

3.4.1 ALERT anonymity protection

ALERT offers identity and site obscurity of the supply and destination, moreover as route obscurity [8]. ALERT makes the route between AN S-D combine troublesome to get by arbitrarily and dynamically choosing the relay nodes. The resultant completely different routes for transmissions between a given SD combine create it troublesome for interloper to watch a applied math pattern of transmission. This is often as a result of the RF set changes because of the random choice of RFs throughout the transmission of every packet. Notwithstanding a mortal detects all the nodes on a route once, this detection don't facilitate it to find the routes for later transmissions between a similar S-D combine.

Additionally, since an RF is merely tuned in to its continuing node and succeeding node in route, the supply and destination nodes cannot be differentiated from alternative nodes on the way. In ALERT, the routes between 2 human activity nodes square measure perpetually dynamical, thus it's troublesome for adversaries to predict the route of successive packet for packet interception. Similarly, the communication of 2 nodes in ALERT cannot be fully stopped by compromising sure nodes as a result of the quantity of doable collaborating nodes in every packet transmission is incredibly giant because of the dynamic route changes.

4. Results and Discussion

The experiments were carried out victimization JAVA with the eclipse tool. Eclipse is AN Integrated Development Tool that provides an in depth model of the physical and link layer behavior of a wireless network and permits capricious movement of nodes at intervals the network. OLSR is AN implementation of Optimized Link State Routing protocol for the JAVA, which complies with and supports all core functionalities of OLSR and the link-layer feedback possibility. The six metrics computed for every simulation run:

i) Packet delivery radio. The quantitative relation between the number of packets originated by the applying layer cosmic radiation (Constant Bit Rate) sources and therefore the number of packets received by the cosmic radiation sink at the ultimate destination.

ii) Routing price. The quantitative relation between the whole bytes of routing packets transmitted throughout the simulation and therefore the total bytes of packets received by the cosmic radiation sink at the ultimate destination.

iii) Packet overhead. The quantity of transmitted routing packets; for instance, a hi or TC message sent over four hops would be counted as four packets during this metric.

iv) Byte overhead. The numbers of transmitted bytes by routing packets, reckoning every hop like Packet Overhead.

v) Mean latency. The typical time march on from “when a knowledge packet is initial sent” to “when it\'s initial received at its destination.”

vi) Average path length. This is often the typical length of the ways discovered by OLSR. it absolutely was calculated by averaging the quantity of hops taken by every knowledge packet to succeed in the destination.

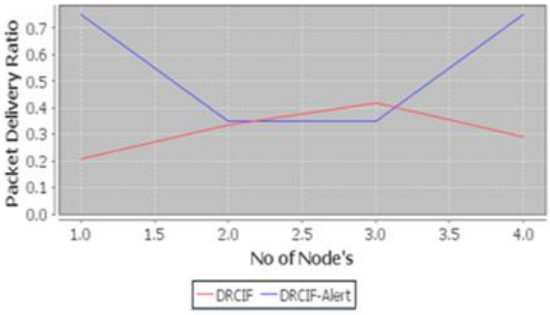

Figure 3: Packet delivery ratio

In Figure 3, because the range of nodes will increase, the packet delivery ratio conjointly will increase as a result of their area unit additional route decisions for the packet transmission. The packets delivery quantitative relation of ALERT is over DRCIF risk-aware response mechanisms.

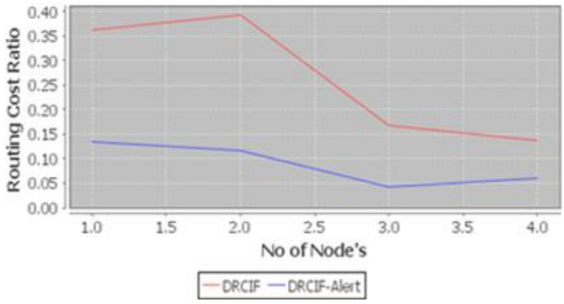

Figure 4: Routing cost

The fluctuations of routing cost shown in Figure 4 are caused by the random traffic generation and random placement of nodes in our realistic simulation. The routing price of ALERT is less than DRCIF risk-aware response mechanisms.

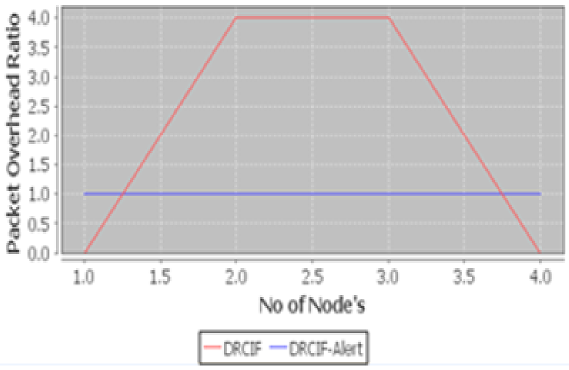

Figure 5: Packet overhead

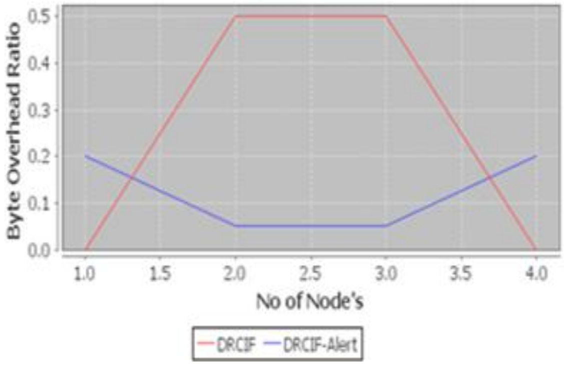

Figure 6: Byte overhead

In ALERT response, the quantity of nodes that isolate the malicious node is a smaller amount than the DRCIF risk-aware response mechanisms. Figure 5 and Figure 6 shows the quantity of nodes will increase, the packet overhead and byte overhead victimization ALERT response area unit slightly over DRCIF risk-aware response mechanisms.

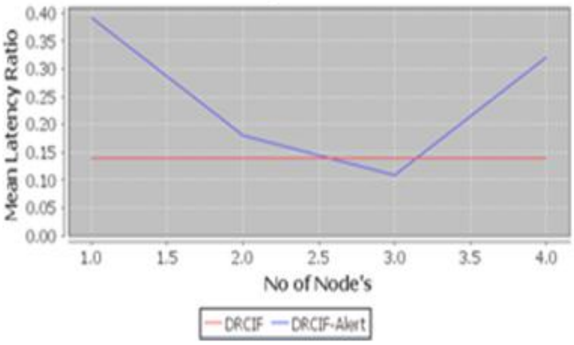

Figure 7: Mean latency

In Figure 7, the mean latency victimization ALERT response is over DRCIF risk-aware response mechanisms, once the quantity of nodes is smaller than twenty. However, once the quantity of nodes is bigger than twenty, the mean latency victimization ALERT approach is a smaller amount than DRCIF risk-aware response mechanisms.

5. Conclusion and future work

The risk-aware response solution for mitigating MANET routing attacks considered the potential damages of attacks and countermeasures. It measures the risk of both attacks and countermeasures using extended Dempster-Shafer theory of evidence. ALERT is distinguished by its low cost and anonymity protection for sources, destinations and routes. It uses dynamic hierarchical zone partitions and random relay node selections to make it difficult for an intruder to detect the two endpoints and nodes en route. A packet in ALERT includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination. In addition ALERT has an efficient solution to counter intersection attacks. Experiment results show that ALERT can offer high anonymity protection at a low cost when compared to other anonymity algorithms.

In Future work applies any secure routing with trust level protocol. Secure Routing using Trust Levels (SRT) scheme in Node transition probability (NTP) protocol to provide secure routing in mobile ad hoc networks based on hierarchical trust levels. In this scheme, the nodes in the network fall into one of the three lists; ally list, associate list and acquaintance list based on the degree of trust.

References

[1] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A.Jamalipour, “A Survey of Routing Attacks in Mobile Ad Hoc Networks,” IEEE Wireless Comm. Magazine, vol. 14, no. 5, pp.85- 91, Oct. 2007.

[2] T. Clausen and P. Jacquet, “Optimized Link State Routing Protocol,” Network Working Group, 2003.

[3] R. Yager, “On the Dempster-Shafer Framework and New Combination Rules_1, Information Sciences,” vol. 41, no. 2, pp.93- 137, 1987.

[4] L. Sun, R. Srivastava, and T. Mock, “An Information Systems Security Risk Assessment Model under the Dempster-Shafer Theory of Belief Functions,” J. Management Information Systems, vol. 22, no. 4, pp. 109-142, 2006

[5] Ziming Zhao, Hongxin Hu, Gail-Joon Ahn, and Ruoyu Wu “Risk-Aware Mitigation for MANET Routing Attack” IEEE Transactions On Dependable And Secure Computing, vol. 9, no. 2, March/April 2012

[6] K. Sentz and S. Ferson, “Combination of Evidence in Dempster- Shafer Theory”, technical report, Sandia Nat’l Laboratories, 2002

[7] Rasha T.K, Shwetha Vincent “A Survey on Intrusion Response Mechanism for MANET Routing Attacks.” International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 2, Issue 10, October 2012)

[8] L. Zhao and H.Shen “Alert: An anonymous location-based efficient routing protocol in Manets.” In *Proc. of ICPP*, 2011.

[9] Y. Sun, W. Yu, Z. Han, and K. Liu, “Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks,” IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 305-317, Feb. 2006

Author Profile

D. Francis Xavier Christopher received his B.Sc., in 1996, M.Sc., in 1998 from Bharathiar University, Coimbatore .He obtained his M.Phil, in the area of Networking from Bharathiar University, Coimbatore in 2002. He submitted his Ph.D thesis. At present he is working as a Director, School of Computer Studies in RVS College of Arts and Science, Coimbatore. His research interest lies in the area of Software Engineering.

R.Nithya received her B.Sc., in 2010, M.Sc., in 2012 from Bharathiar University, Coimbatore. At present she is pursuing her M.Phil in the area of Networking in RVS College of Arts and Science, Coimbatore.